Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1060

(06/2021)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de la información y de las redes – Gestión de la seguridad

Marco para la creación y operación de un centro de ciberdefensa

Recomendación UIT-T X.1060

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	**X.1050–X.1069**
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
SEGURIDAD DE 5G	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1060

Marco para la creación y operación de un centro de ciberdefensa

Resumen

La Recomendación UIT-T X.1060 define el centro de ciberdefensa (CCD) como una entidad que desempeña un papel fundamental en toda organización para hacer frente a los riesgos de ciberseguridad. El marco describe los tres procesos que el CCD debe aplicar en la práctica, a saber, construcción, gestión y evaluación. También se indican los servicios que debe prestar la organización para aplicar medidas de ciberseguridad más específicas.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1060	2021-06-29	17	11.1002/1000/14721

Palabras clave

Centro de ciberdefensa, centro de operaciones de seguridad (COS), EIII.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT [no] ha recibido notificación de la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT T disponibles en el sitio web del UIT T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Introducción

Los riesgos de ciberseguridad en una organización repercuten considerablemente en el conjunto de sus actividades. Los riesgos a los que se enfrentan las organizaciones se derivan de los cambios de su entorno, tanto desde el punto de vista social como empresarial, y de las presiones externas que ejerce la reglamentación y los peligros crecientes. Por consiguiente, la alta dirección, es decir los cargos directivos (CxO), es responsable de gestionar los controles de toda la organización para responder a dichos riesgos y cambios. Un aspecto importante a la hora de aplicar controles en el ámbito de la ciberseguridad es orientar el desarrollo y control de las políticas de seguridad en consonancia con los objetivos empresariales, tarea que suele recaer en el Jefe de Seguridad (CSO) o Jefe de Seguridad de la Información (CISO). Para aplicar las medidas de seguridad resulta indispensable contar con una entidad que ejecute las actividades del CSO o CISO con una gestión estratégica a nivel de la organización. Esta entidad se denomina centro de ciberdefensa (CCD) en esta Recomendación.

En la presente Recomendación se describe un marco para la construcción y gestión de un CCD, así como para evaluar su eficacia. El marco indica cómo el CCD debe determinar e implementar los servicios de seguridad para lograr la seguridad de la organización. Este marco ayuda a la organización a abordar sus riesgos de ciberseguridad.

Recomendación UIT-T X.1060

Marco para la creación y operación de un centro de ciberdefensa

1 Alcance

En esta Recomendación se presenta un marco para que las organizaciones construyan y gestionen un centro de ciberdefensa (CCD) y evalúen su eficacia. El marco indica cómo el CCD debe determinar e implementar los servicios de seguridad para lograr la seguridad de una organización.

Esta Recomendación está destinada a los altos directivos responsables de la seguridad de una organización, ya sea el Jefe de Seguridad (CSO) o Jefe de Seguridad de la Información (CISO) y los supervisores de seguridad que les asisten.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 externalización [b-ITU-T X.1053]: Cuando una empresa subcontrata uno o varios de sus procesos y/o funciones internas a una empresa externa. La subcontratación transfiere los recursos de la empresa a una empresa externa y mantiene cierta capacidad para gestionar la relación con los procesos subcontratados.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 centro de ciberdefensa (CCD): Entidad de la organización que ofrece servicios de seguridad para gestionar los riesgos de ciberseguridad que acechan a su actividad empresarial.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siguientes siglas y acrónimos:

APT Amenaza persistente avanzada

CCD Centro de Ciberdefensa

CISO Jefe de seguridad de la información

CSIRT Equipo de intervención en caso de incidente de seguridad informática

CSO Jefe de seguridad

CxO Cargos directivos (*C-suite*)

IDS Sistema de detección de intrusión

IPS Sistema de prevención de intrusión

IT Tecnología de la información

SIEM Gestión de información y eventos de seguridad

SLA Acuerdo de nivel de servicio

WAF Cortafuegos de aplicaciones web

5 Convenios

Ninguno.

6 Estructura de la Recomendación

En la cláusula 7 de la presente Recomendación se explica el concepto de CCD. En la cláusula 8 se describe el marco para la creación y operación del CCD. El marco se describe en detalle en las cláusulas subsiguientes: proceso de construcción del CCD (cláusula 9); proceso de gestión del CCD (cláusula 10); y proceso de evaluación del CCD (cláusula 11). En la cláusula 12 se presenta, a título de práctica idónea, una descripción general de los servicios de seguridad proporcionados por la CCD, y en el Anexo A se describe en detalle cada uno de esos servicios.

7 Descripción del centro de ciberdefensa

Las organizaciones tienen por objeto lograr el éxito de sus negocios. Para gestionar los riesgos de la actividad empresarial, el CISO formula políticas de seguridad, especialmente desde la perspectiva de la ciberseguridad. El CCD es una entidad que ejecuta las políticas de seguridad mediante servicios específicos del CCD, que consisten en actividades de seguridad que realizan los equipos encargados de la seguridad. Los servicios CCD especifican las funciones de seguridad en forma de capacidades del sistema para realizar procesos relacionados con la seguridad. La Figura 1 muestra los distintos actores y sus funciones para el funcionamiento de los CCD.

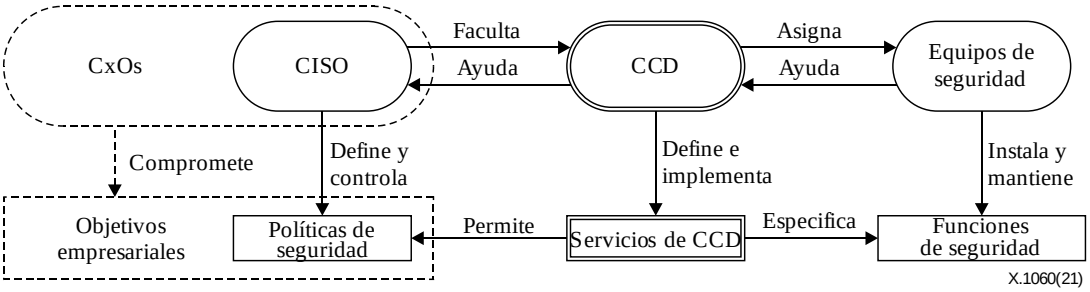

Figura 1 – Distintos actores y sus funciones en el funcionamiento del CCD

Dependiendo del tamaño y del tipo de organización, el CCD puede ser una unidad independiente, un comité o un pequeño equipo. Más allá de su formato, es indispensable que este centro exista en el seno de la organización y cuente con la autoridad y los recursos necesarios para poner en marcha servicios de seguridad que permitan garantizar la seguridad de la organización. Dichos servicios de seguridad deben estar en consonancia con las políticas de seguridad y garantizar la calidad de las actividades de seguridad; el nivel de cada servicio debe estar explícitamente acordado en un documento, por ejemplo, en un acuerdo de nivel de servicio (SLA). La calidad general de un servicio de seguridad CCD se evalúa mediante las medidas especificadas en la cláusula 9.4.

8 Marco para la creación y operación del CCD

La Figura 2 ilustra un marco para la creación y explotación de un CCD. El marco incluye tres procesos: creación, gestión y evaluación. Para garantizar la seguridad de la organización, el CCD se debe crear y gestionar adecuadamente. Además, es preciso evaluarlo de forma oportuna y periódica y mejorarlo continuamente. Este marco permite a la organización realizar las actividades de seguridad.

En el proceso de construcción deben tenerse en cuenta las actividades de seguridad de la organización. Las prácticas idóneas para los servicios de seguridad de los CCD se enumeran en el Anexo A. Cada organización puede confeccionar su propio catálogo de servicios utilizando para ello la lista y añadiendo los servicios específicos que estime oportunos. Para cada servicio del catálogo se debe establecer también un perfil que incluya: el titular o titulares, las funciones y responsabilidades, y el tipo de asignación de servicios (internos, externos o mixtos). Una vez establecido el perfil del servicio, debe determinarse el peso actual y deseado de cada servicio del CCD para el proceso de evaluación.

El proceso de gestión consta de tres fases y dos ciclos. En la fase de gestión estratégica se gestiona las actividades generales del CCD, en la fase de explotación se gestiona el trabajo rutinario de supervisión y análisis, y en la fase de respuesta se gestiona la intervención en caso de emergencia. Estas fases se gestionan en ciclos cortos y largos, según proceda; en las fases de explotación y de respuesta se precisan resoluciones inmediatas en ciclos cortos. En cambio, en la fase de gestión estratégica se debe analizar las mejoras a largo plazo e incorporar los resultados de los ciclos cortos en un ciclo largo. Por lo general, para introducir mejoras a largo plazo hay que tomar decisiones sobre nuevas inversiones empresariales y modificar drásticamente las arquitecturas de los sistemas.

En la evaluación se valoran el catálogo, el perfil y la cartera de un servicio de CCD (véase la Figura 4), que deben evaluarse objetivamente en cada momento.

Los resultados de la evaluación se deben revisar y plasmar en los tres procesos de CCD. Hay que establecer y mantener en la organización un ciclo recurrente de los procesos de construcción, gestión y evaluación para mejorar las actividades de seguridad.

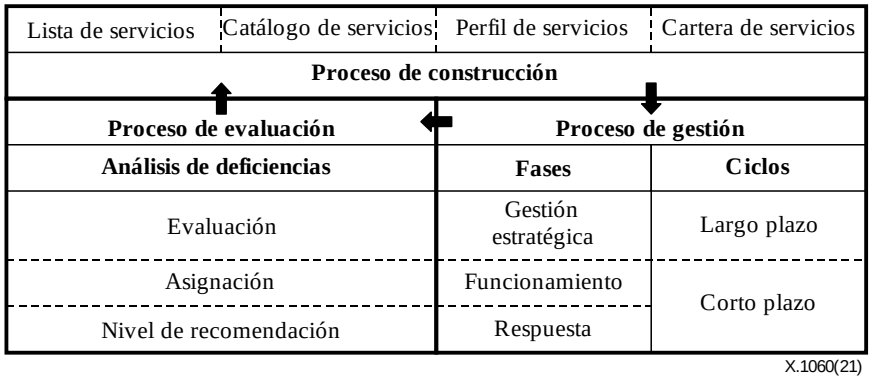

Figura 2 – Marco para la creación y explotación del CCD

9 Proceso de construcción

9.1 Generalidades

En el proceso de construcción del CCD se ha de determinar qué servicios de seguridad se requiere aplicar en la organización. Los posibles servicios se seleccionan de entre la lista de servicios del CCD, basada en la práctica idónea en la organización. En la cláusula 12 se puede consultar la lista de servicios del CCD.

La Figura 3 muestra las tres fases de construcción de servicios del CCD.

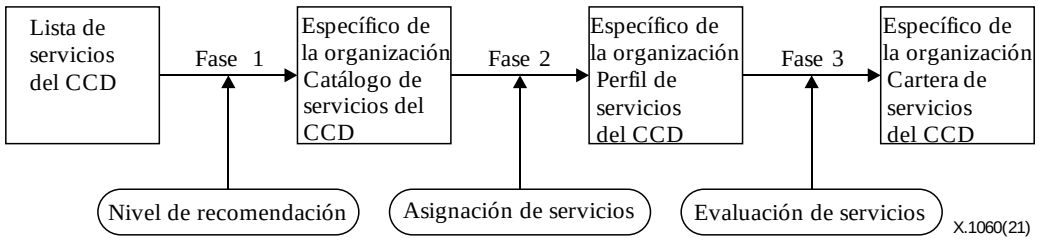

Figura 3 – Fases para la construcción de servicios del CCD

1) Fase 1: Creación de un catálogo de servicios del CCD

En primer lugar, la organización debe crear un catálogo de servicios del CCD.

En esta fase, los servicios posibles para su prestación se extraen de la lista de servicios generales. La lista general se describe detalladamente en la cláusula 12. Si faltara alguno de estos servicios, se podrán definir y añadir nuevos servicios al catálogo de servicios del CCD.

2) Fase 2: Creación de un perfil de servicio del CCD

Para los servicios enumerados en el catálogo de servicios CCD, la organización debe determinar las funciones y responsabilidades de equipos que prestan esos servicios. En esta fase, se han de tener en cuenta la asignación de servicios del CCD descrita en la cláusula 9.3.

Así, la organización debe elaborar el perfil de servicios del CCD.

3) Fase 3: Creación del perfil de servicios del CCD

Una vez decidido el perfil de servicios del CCD, la organización debe medir la actual puntuación de servicios (presente) de cada servicio y establecer la puntuación deseada del servicio a medio o largo plazo (futura).

Una vez definidos los niveles presentes y futuros, la organización debe elaborar la cartera de servicios del CCD.

La Figura 4 muestra una matriz de ejemplo de servicios CCD. Esta matriz debe completarse después de las fases 1 a 3.

Servicio	Nivel de recomendación	Asignación de servicios	Puntuación del servicio	
			Actual	Futuro
Ej. servicio1	Básico	Recursos internos (Dept. AB)	3	5
Ej. servicio 2	Normal	Externalización (Z-MSSP)	2	4
Ej. servicio 3	Avanzado	No asignable	1	2

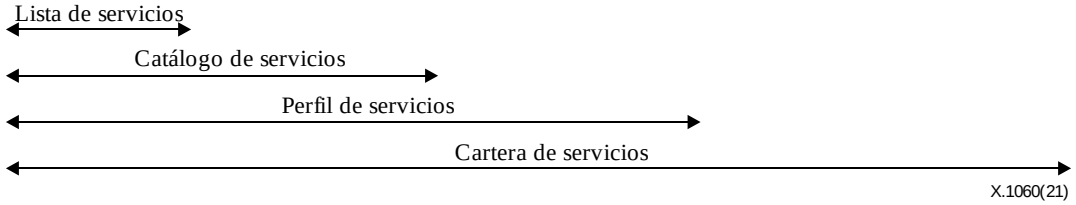

Figura 4 – Matriz de servicios del CCD

9.2 Nivel de recomendación de servicios del CCD

Para poner en marcha los servicios del CCD más adecuados para la organización, se debe considerar la necesidad de cada servicio en los cinco niveles indicados en el Cuadro 1. La prioridad de cada servicio en lo que respecta a su puesta en marcha debe aclararse midiendo los niveles.

Cuadro 1 – Nivel de recomendación de los servicios CCD

Ponderación	Descripción
Innecesario	Servicios considerados innecesarios
Básico	Servicios mínimos que se pretenden poner en marcha
Normal	Servicios cuya puesta en marcha generalmente se recomienda
Avanzado	Servicios necesarios para alcanzar el ciclo CCD de mayor nivel
Opcional	Servicios seleccionados arbitrariamente según la forma esperada del CCD

9.3 Asignación de servicios del CCD

La organización debe aclarar específicamente qué equipo se encargará de prestar el servicio CCD. Dependiendo de las capacidades de prestación de servicios, la organización debe determinar la asignación de servicios del CCD que pudieran externalizarse. Véase el Cuadro 2.

Cuadro 2 – Asignación de servicios del CCD

Tipo	Descripción
Recursos internos	Los servicios los presta un equipo interno de la organización. Ésta debe especificar el equipo encargado
Externalización	Los servicios los presta un equipo externo a la organización. Ésta debe especificar a quién se externaliza
Combinación	La organización recurre tanto recursos internos como a la externalización. La organización de especificar el equipo responsable y el contratista
No asignado	Aunque la organización presta el servicio, no han nadie asignado en la organización

Cuando se recurre a la externalización, los puntos A) y B) deben aclararse.

A) Naturaleza de la información gestionada

La organización debe clasificar la naturaleza de la información gestionada, incluidas las definiciones o distinciones entre "interna" y "externa" a la organización. Por ejemplo, en caso de incidente, la información sobre los daños o efectos causados por el ataque debe considerarse interna, mientras que la información sobre el ataque propiamente dicho se considerará externa.

B) Necesidad de conocimientos especializados en materia de seguridad

La organización debe analizar si se requieren conocimientos especializados en el campo de la seguridad para prestar el servicio.

Los servicios de CCD se clasifican en los cuadrantes I) a IV) basados en dos puntos de indicadores. Véase la Figura 5.

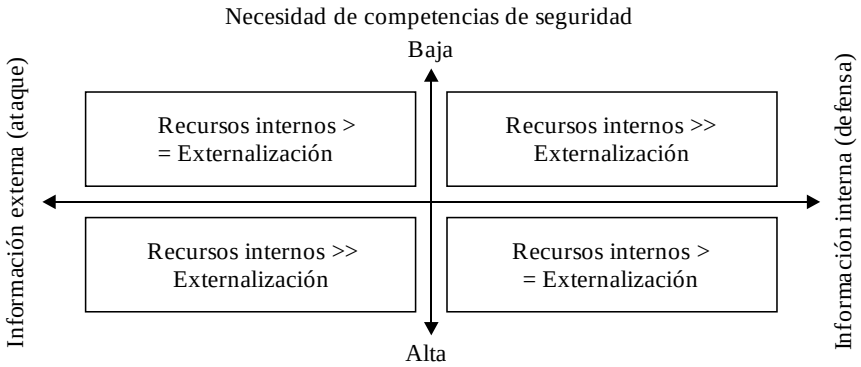

Figura 5 – Cuadrantes de contratación

I) Recursos internos >> Externalización

Cuando no se precisan conocimientos técnicos de seguridad para gestionar la información confidencial dentro de la organización, la utilización de recursos internos es la solución óptima por lo que no se requiere recurrir a la externalización.

II) Recursos internos >= Externalización

Cuando no se requieren un nivel de conocimientos elevado, aunque sea información externa a la organización, tanto la actividad como la gestión debe realizarse internamente por la organización con apoyo externo.

III) Recursos internos << Externalización

Para tratar la información externa a la organización, principalmente la relativa a los ataques, la organización encargada de prestar ese servicio debe disponer de conocimientos especializados (por ejemplo, recurrir a la externalización). A menos que la organización disponga internamente de expertos con conocimientos especializados, será difícil que pueda prestar el servicio.

IV) Recursos internos <= Externalización

Cuando se requieran conocimientos especializados para gestionar la información interna de una organización, la actividad debe ser realizada principalmente por una entidad especializada (por ejemplo, recurriendo a la externalización), que la organización debe gestionar y apoyar.

9.4 Evaluación del servicio del CCD

Cuando se crea la cartera de servicios del CCD, el estado actual y futuro de cada servicio debe evaluarse utilizando las puntuaciones de los servicios que figuran en el Cuadro 3. Cabe señalar que los distintos tipos de servicios, por ejemplo, los que se contratan internamente y los que se externalizan, deben evaluarse según los criterios asignados a las puntuaciones de los servicios.

Cuadro 3 – Puntuación de los servicios del CCD

Servicios internos	
El CISO u otro director de la organización con potestad para ello autoriza la explotación, que está documentada	+5 puntos
La explotación está documentada y otros actores pueden desempeñar la función del operador existente	+4 puntos
La explotación no está documentada y otros puede desempeñar parcialmente la función del operador existente de una manera temporal	+3 puntos
La explotación no está documentada y el operador existente puede desempeñar la función	+2 puntos
La explotación no está funcionando	+1 punto
Se decide no prestar el servicio con recursos internos	–
El contenido del servicio y los resultados esperados se comprenden y sus resultados son los esperados	+5 puntos
El contenido del servicio y los resultados esperados se comprenden, pero sus resultados no son los esperados	+4 puntos

Cuadro 3 – Puntuación de los servicios del CCD

Servicios externalizados	
El contenido del servicio o los resultados esperados no se comprenden	+3 puntos
Ni el contenido del servicio ni los resultados esperados no se comprenden	+2 puntos
Ni los resultados ni el informe se examinan	+1 punto
Se decide no prestar el servicio con externalización	–

10 Proceso de gestión

El CCD realiza actividades de seguridad en toda la organización mediante el proceso de gestión del CCD que consta de tres fases y dos ciclos, como ilustra la Figura 6.

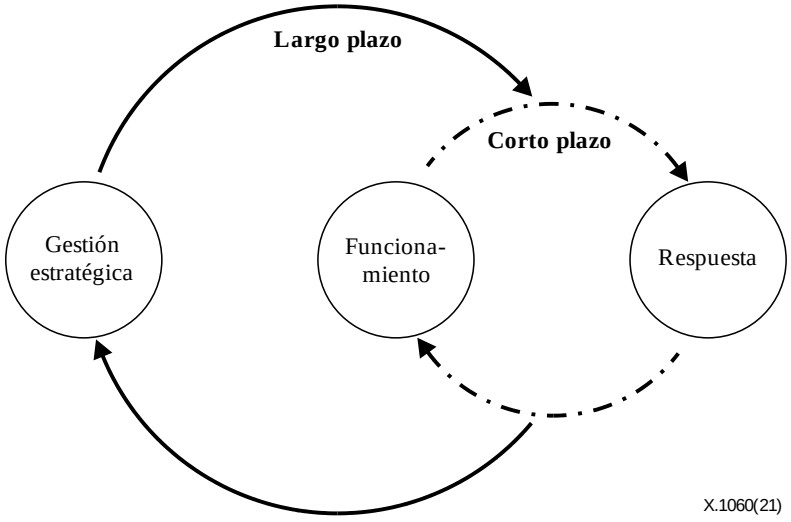

Figura 6 – Proceso de gestión del CCD

1) Fase de gestión estratégica

La gestión estratégica se encarga de todos los servicios estratégicos relacionados con las definiciones, el diseño, la planificación, la gestión, la certificación, etc., que garantizan la evolución a largo plazo de CCD.

2) Fase de explotación

El mantenimiento del marco instaurado debe realizarse en la fase de explotación. Consiste en el trabajo cotidiano y habitual y suele incluir actividades ordinarias como, por ejemplo, el análisis de la detección de incidentes y la supervisión y el mantenimiento de los sistemas de respuesta de seguridad. El equipo encargado de estas operaciones suele denominarse centro de operaciones de seguridad (SOC).

3) Fase de respuesta

La respuesta a incidentes debe ejecutarse cuando se detecta un evento en la fase de explotación. Esta fase siempre se considera una emergencia. El equipo que reacciona ante el incidente suele denominarse equipo de intervención en caso de incidente de seguridad informática (EIISI).

Durante la fase de respuesta, el equipo no debe basarse exclusivamente en los datos obtenidos en la fase de explotación, sino que también debe tener en cuenta las respuestas a los informes o notificaciones de terceros.

A) Corto plazo

La explotación y la respuesta se realizan a diario. En estos procesos, siempre aparecen problemas operativos y problemas en el sistema de respuesta de seguridad. Por consiguiente, resulta imprescindible mejorar continuamente estos sistemas para resolver esos problemas, por ejemplo, la simple automatización de tareas sencillas, la mejora de las herramientas para analizar la precisión y la revisión de los elementos de los informes, dentro de los recursos (personas, presupuesto, sistema) asignados a corto plazo.

B) Largo plazo

Toda revisión que requiera la asignación de nuevos recursos debe aplicarse a largo plazo.

Si al revisar los planes a corto plazo se determina que no se pueden resolver los problemas con el sistema actual, habrá que aplicar una perspectiva y un plan a largo plazo, por ejemplo, mediante la introducción de un nuevo producto de seguridad, la revisión drástica de las políticas de seguridad y el cambio de configuración a gran escala en los sistemas de seguridad.

11 Proceso de evaluación

11.1 Generalidades

$$

El catálogo, perfil y cartera de servicios del CCD que se formulan en el proceso de construcción deben evaluarse periódica y regularmente. La Figura 7 ilustra el proceso de evaluación de los servicios CCD.

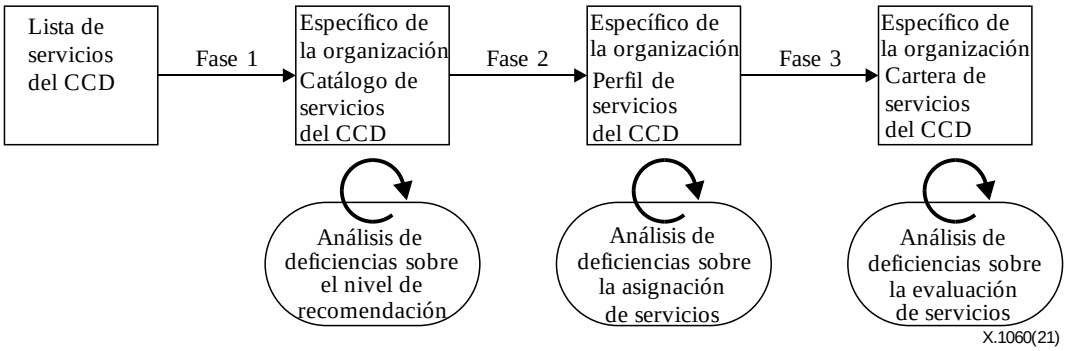

Figura 7 – Proceso de evaluación del CCD

11.2 Evaluación del catálogo de servicios del CCD

Se ha de analizar las deficiencias a nivel de recomendación de servicios del CCD. Es necesario revisar los servicios debido a los cambios en el entorno y los peligros, en particular, los considerados "innecesarios" se han de reexaminar y revisar para garantizar que no haya omisiones. Cada vez que la empresa introduzca cambios, se habrá de evaluar el catálogo de servicios CCD, por ejemplo, cuando inicie nuevas actividades comerciales, y responder a los nuevos riesgos y amenazas.

11.3 Evaluación del perfil de servicios del CCD

Se ha de analizar las deficiencias en las asignaciones de servicios del CCD. Al decidir las asignaciones de servicios, se pueden eliminar los "no asignables", y la organización puede esperar mejorar el nivel de madurez al revisarlos. El perfil de servicio CCD debe evaluarse cuando se produzcan cambios en la organización, como por ejemplo cambios internos para servicios con recursos internos y cambios de la entidad externa en caso de externalización.

11.4 Evaluación de la cartera de servicios del CCD

Se ha de analizar las deficiencias en la puntuación de cada uno de los servicios del CCD. Debe aclararse la diferencia entre la puntuación futura prevista y la actual para que la organización pueda concentrarse en lo que hay ha de mejorar, confirmar de nuevo la puntuación del servicio CCD y determinar los problemas. La cartera de servicios del CCD debe evaluarse periódicamente.

12 Categorías de servicios y lista de servicios del CCD

Las categorías y la lista de servicios del CCD son necesarios en los procesos de construcción y gestión (véanse las cláusulas 9 y 10).

Los servicios del CCD se dividen en nueve categorías:

A) Gestión estratégica del CCD;

B) Análisis en tiempo real;

C) Análisis profundo;

D) Respuesta a incidentes;

E) Verificación y evaluación;

F) Recopilación, análisis y evaluación de la inteligencia de las amenazas;

G) Desarrollo y mantenimiento de plataformas del CCD;

H) ayuda a la respuesta contra el fraude interno;

I) Relación activa con partes externas.

A. Gestión estratégica del CCD

Esta categoría incluye la planificación de políticas y recursos para todas las actividades relacionadas con la seguridad mencionadas en las categorías A) a I) de la organización, en particular el CCD para garantizar su funcionamiento estable.

B. Análisis en tiempo real

Esta categoría consiste en supervisar y analizar los registros y los datos de diversos sistemas, como los dispositivos de red, los servidores y los productos de seguridad. La meta es detectar las amenazas en tiempo real, que pueden dar lugar a una respuesta rápida y adecuada a los incidentes.

C. Análisis profundo

Esta categoría está relacionada con los incidentes, por ejemplo, la investigación de los sistemas afectados, el examen de los datos filtrados y la herramientas y métodos de análisis utilizados en el ataque.

La finalidad es elucidar el alcance global del incidente e identificar su repercusión.

D. Respuesta a incidentes

Esta categoría se refiere a las actuaciones concretas resultantes del análisis en tiempo real y de la información sobre amenazas para disuadirlas y eliminarlas.

El objetivo es minimizar la incidencia en el sistema y la actividad económica, en particular la coordinación y notificación a otras partes interesadas.

E. Verificación y evaluación

Esta categoría se refiere a la evaluación de la vulnerabilidad de sistemas que se ha de proteger, la formación en respuesta a incidentes y su evaluación. La finalidad es mejorar el nivel de seguridad.

F. Recopilación, análisis y evaluación de la inteligencia de amenazas

Esta categoría se refiere a la recopilación de información sobre vulnerabilidades y ataques (inteligencia externa) que está disponible en Internet y a la gestión de la información mediante análisis de tiempo real y respuesta a incidentes (inteligencia interna).

El objetivo es mejorar la precisión del análisis en tiempo real y la respuesta a incidentes, así como mejorar los activos de seguridad.

G. Desarrollo y mantenimiento de plataformas CCD

Esta categoría se refiere a la gestión, mejora o desarrollo de nuevos sistemas (por ejemplo, productos de seguridad, bases de datos de recopilación de registros y sistemas operativos) que son necesarios para la respuesta de seguridad.

La finalidad es lograr el desempeño eficaz y sostenible de las otras categorías.

H. Ayuda a la respuesta contra el fraude interno

Esta categoría se refiere a la recopilación de datos de auditoría para ayudar a responder al fraude interno.

La finalidad es ayudar a responder y resolver los casos de fraude interno mediante el suministro de registros y análisis.

I. Relación activa con partes externas

Esta categoría incluye la coordinación y colaboración con actores internos y organizaciones externas.

El objetivo es mejorar el nivel de seguridad de la organización, aumentar el valor de la seguridad para la organización y, así, reforzar y desarrollar la organización.

La Figura 8 muestra la relación de las categorías de servicio con los procesos de gestión, y en el Cuadro 4 se enumera los servicios.

En el Anexo A figura una descripción detallada de cada servicio de la lista de servicios del CCD.

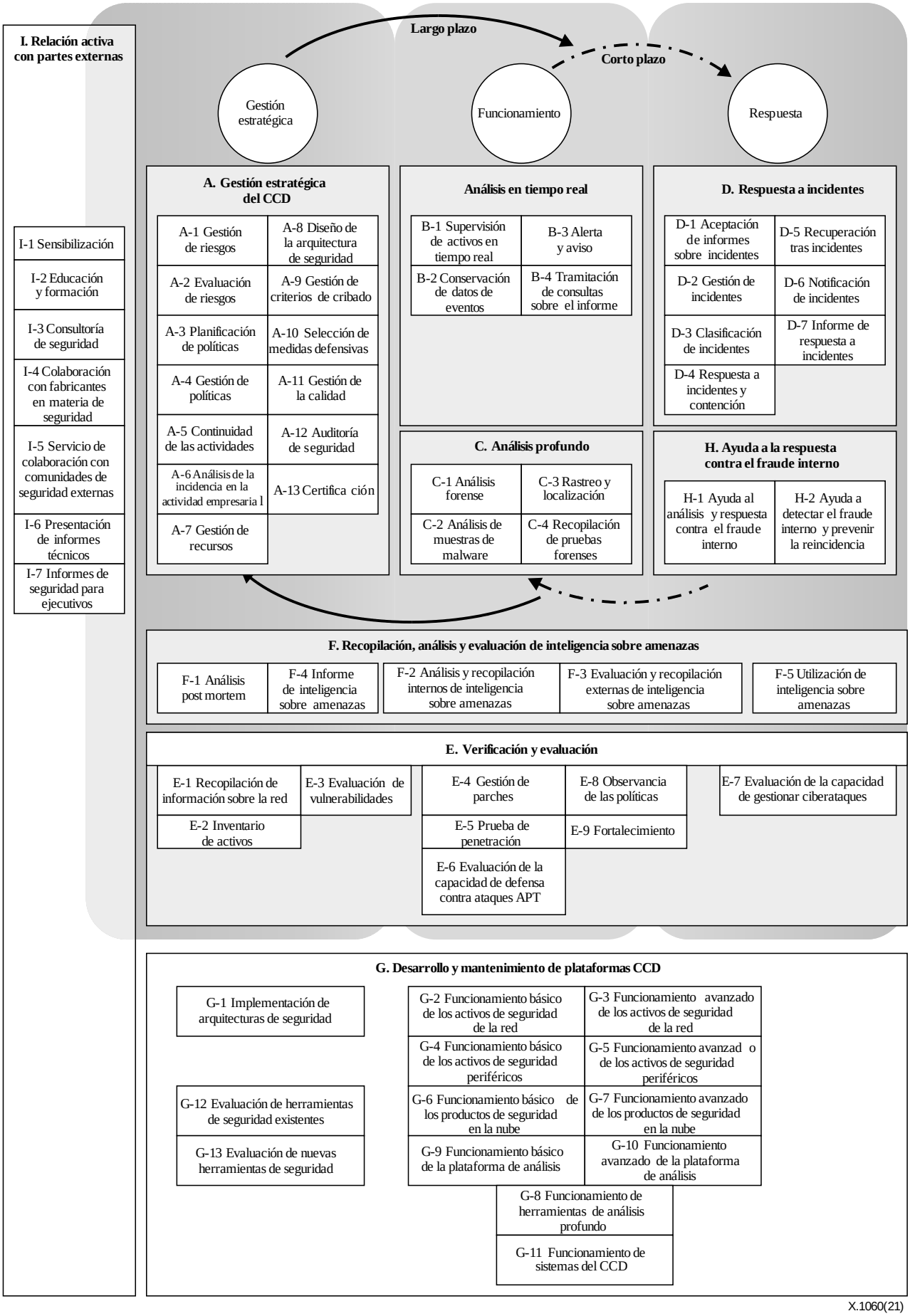

Figura 8 – Categorías de servicios del CCD

Cuadro 4 – Lista de servicios del CCD

A.	**Gestión estratégica del CCD**	**F.**	**Recopilación, análisis y evaluación de inteligencia sobre amenazas**
A-1	Gestión de riesgos	F-1	Análisis *post mortem*
A-2	Evaluación de riesgos	F-2	Análisis y recopilación internos de inteligencia sobre amenazas
A-3	Planificación de políticas	F-3	Evaluación y recopilación externas de inteligencia sobre amenazas
A-4	Gestión de políticas	F-4	Informe de inteligencia sobre amenazas
A-5	Continuidad de las actividades	F-5	Utilización de inteligencia sobre amenazas
A-6	Análisis de la incidencia en la actividad empresarial	**G.**	**Desarrollo y mantenimiento de plataformas CCD**
A-7	Gestión de recursos	G-1	Implementación de arquitecturas de seguridad
A-8	Diseño de la arquitectura de seguridad	G-2	Funcionamiento básico de los activos de seguridad de la red
A-9	Gestión de criterios de cribado	G-3	Funcionamiento avanzado de los activos de seguridad de la red
A-10	Selección de medidas defensivas	G-4	Funcionamiento básico de los activos de seguridad periféricos
A-11	Gestión de la calidad	G-5	Funcionamiento avanzado de los activos de seguridad periféricos
A-12	Auditoría de seguridad	G-6	Funcionamiento básico de los productos de seguridad en la nube
A-13	Certificación	G-7	Funcionamiento avanzado de los productos de seguridad en la nube
B.	**Análisis en tiempo real**	G-8	Funcionamiento de herramientas de análisis profundo
B-1	Supervisión de activos en tiempo real	G-9	Funcionamiento básico de la plataforma de análisis
B-2	Conservación de datos de eventos	G-10	Funcionamiento avanzado de la plataforma de análisis
B-3	Alerta y aviso	G-11	Funcionamiento de sistemas del CCD
B-4	Tramitación de consultas sobre el informe	G-12	Evaluación de herramientas de seguridad existentes
C.	**Análisis profundo**	G-13	Evaluación de nuevas herramientas de seguridad
C-1	Análisis forense	**H.**	**Ayuda a la respuesta contra el fraude interno**
C-2	Análisis de muestras de malware	H-1	Ayuda al análisis y respuesta contra el fraude interno
C-3	Rastreo y localización	H-2	Ayuda a detectar el fraude interno y prevenir la reincidencia
C-4	Recopilación de pruebas forenses	**I.**	**Relación activa con partes externas**
D.	**Respuesta a incidentes**	I-1	Sensibilización
D-1	Aceptación de informes sobre incidentes	I-2	Educación y formación
D-2	Gestión de incidentes	I-3	Consultoría de seguridad

Cuadro 4 – Lista de servicios del CCD

D-3	Clasificación de incidentes	I-4	Colaboración con fabricantes en materia de seguridad
D-4	Respuesta a incidentes y contención	I-5	Servicio de colaboración con comunidades de seguridad externas
D-5	Recuperación tras incidentes	I-6	Presentación de informes técnicos
D-6	Notificación de incidentes	I-7	Informes de seguridad para ejecutivos
D-7	Informe de respuesta a incidentes		
E.	**Verificación y evaluación**		
E-1	Recopilación de información sobre la red		
E-2	Inventario de activos		
E-3	Evaluación de vulnerabilidades		
E-4	Gestión de parches		
E-5	Prueba de penetración		
E-6	Evaluación de la capacidad de defensa contra ataques APT		
E-7	Evaluación de la capacidad de gestionar ciberataques		
E-8	Observancia de las políticas		
E-9	Fortalecimiento		

Anexo A

Lista de servicios del CCD con su descripción

(Este anexo forma parte integrante de la presente Recomendación.)

A.1 Categoría A: Gestión estratégica del CCD

A.1.1 A-1. Gestión de riesgos

El servicio de gestión de riesgos consiste en coordinar las actividades A-2 a A-13 para orientar y controlar la organización en lo relativo a los riesgos.

A.1.2 A-2. Evaluación de riesgos

El servicio de evaluación de riesgos describe la situación actual del nivel de riesgo de la organización en cuanto a activas, amenazas y medidas de seguridad.

A.1.3 A-3. Planificación de políticas

El servicio de planificación de políticas da soporte a todas las actividades para la definición de políticas y recopilación de directrices.

A.1.4 A-4. Gestión de políticas

El servicio de gestión de políticas tiene por objeto realizar exámenes periódicos para evaluar políticas y reglas de la organización, a fin de cumplir requisitos nuevos o externos (por ejemplo, reglamentos y directrices).

A.1.5 A-5. Continuidad de las actividades

El servicio de continuidad de la actividad contribuye a las funciones operativas necesarias para garantizar la aplicación y ejecución adecuadas del plan de continuidad de las actividades de la organización.

A.1.6 A-6. Análisis de la incidencia en la actividad empresarial

El servicio de análisis de la incidencia en la actividad empresarial tiene por objeto evaluar sistemáticamente las posibles repercusiones de los diversos eventos o situaciones. Este servicio contribuye a comprender la magnitud de las pérdidas que podrían producirse. Además de las pérdidas económicas directas, también considera otras repercusiones, como la pérdida de la confianza de sus partes interesadas y el perjuicio a la reputación.

A.1.7 A-7. Gestión de recursos

El servicio de gestión de recursos planifica los recursos (personal, presupuesto, sistemas, etc.) para dar soporte a las actividades de seguridad y atribuirlas adecuadamente a cada servicio.

A.1.8 A-8. Diseño de la arquitectura de seguridad

El servicio de diseño de la arquitectura de seguridad tiene por objeto establecer la arquitectura para proteger la actividad empresarial. El desarrollo y mantenimiento de plataformas CCD (categoría G) puede lograrse mediante la recopilación de diversas medidas de seguridad que tienen en cuenta el diseño de sistemas y las restricciones de los procesos empresariales (por ejemplo, la cadena de suministro).

A.1.9 A-9. Gestión de criterios de cribado

El servicio de gestión de criterios de cribado tiene por objeto especificar los criterios de cribado (prioridad de respuesta) para eventos (por ejemplo, incidentes, vulnerabilidades detectadas, información sobre amenaces recabada) en el marco de la política general acordada.

A.1.10 A-10. Selección de medidas defensivas

El servicio de selección de medidas defensivas tiene por objeto dar soporte a todas las actividades de selección de medidas defensivas con arreglo a los criterios de cribado (A-9) y seleccionar las mejores tecnologías para todas las disposiciones de seguridad.

A.1.11 A-11. Gestión de la calidad

El servicio de gestión de la calidad tiene por objeto verificar los problemas de calidad en las actividades relacionadas con la seguridad, tengan o no un efecto negativo para las actividades (por ejemplo, utilidad, productividad) a lo largo de un periodo de tiempo (por ejemplo, una semana o un mes).

A.1.12 A-12. Auditoría de seguridad

El servicio de auditoría de seguridad verifica sistemática y cuantificablemente cómo aplica la organización las políticas y controles de seguridad en un determinado emplazamiento o instante. El personal del CCD participa indirectamente en las actividades de auditoría proporcionando la información y las pruebas necesarias para la situación de control vigentes.

A.1.13 A-13. Certificación

El servicio de certificación da soporte a las actividades necesarias para que la organización cumpla diversas normas y sistemas de certificación.

A.2 Categoría B: Análisis en tiempo real

A.2.1 B-1. Supervisión de activos en tiempo real

El servicio de supervisión de activos en tiempo real tiene por objeto supervisar y analizar el estado de los sistemas o las actividades sospechosas a partir de los registros y los flujos de red, y colabora en el cribado cuando se requiere recopilar información sobre un incidente o evento.

A.2.2 B-2. Conservación de datos de eventos

El servicio de retención de datos de eventos recopila y almacena de manera centralizada los eventos recabados en el proceso de supervisión y análisis de seguridad.

A.2.3 B-3. Alerta y aviso

El servicio de alerta y aviso tiene por objeto notificar la función interna implicada en los eventos que suponen un riesgo potencial para los activos de información (por ejemplo, alerta de dispositivos de seguridad, boletines de seguridad, vulnerabilidades y propagación de amenazas).

A.2.4 B-4. Tramitación de consultas sobre informes

La tramitación de consultas sobre el servicio de notificación tiene por objeto responder a las preguntas sobre datos e informes relativos a los análisis.

A.3 Categoría C: Análisis profundo

A.3.1 C-1. Análisis forense

El servicio de análisis forense consiste en analizar las pruebas digitales recopiladas a partir de los activos de seguridad en relación con un evento a fin de ayudar a determinar lo sucedido.

A.3.2 C-2. Análisis de muestras de malware

El servicio de análisis de muestras de malware tiene por objeto analizar el malware, los programas o las secuencias de instrucciones desplegados por los atacantes que se encuentran en cada análisis forense.

A.3.3 C-3. Rastreo y localización

Este servicio constituye la capacidad de una organización para rastrear y localizar el origen de cualquier ataque a sus infraestructuras, lo que resulta esencial a la hora de reducir nuevas incidencias y prevenir incidentes de seguridad. La capacidad reconocida de rastrear y localizar a los atacantes tanto internos como externos (por ejemplo, la ciberatribución) permite prevenir futuros ataques.

A.3.4 C-4. Recopilación de pruebas forenses

El servicio de recopilación de pruebas forenses consiste en recabar y conservar pruebas electrónicas digitales relativas a un incidente objeto de investigación y elaborar y mantener la validez de las pruebas ("cadena de custodia de las pruebas").

A.4 Categoría D: Respuesta a incidentes

A.4.1 D-1. Aceptación de informes sobre incidentes

El servicio de aceptación de informes sobre incidentes tiene por objeto recibir informes analíticos de operaciones. Ahora bien, también puede recibir informes de otras organizaciones de la misma empresa o de organizaciones externas.

A.4.2 D-2. Gestión de incidentes

El servicio de gestión de incidentes tiene por objeto gestionar los incidentes aceptados y coordinar las actividades, en particular las D-3 a D-7.

A.4.3 D-3. Clasificación de incidentes

El servicio de clasificación de incidentes tiene por objeto clasificar los incidentes para contribuir a un entendimiento común de los tipos de incidentes que se producen y cuáles son sus causas.

A.4.4 D-4. Respuesta a incidentes y contención

El servicio de respuesta a incidentes y contención tiene por objeto evitar incidentes antes de que se propaguen por todos los recursos y aumenten los daños o su incidencia.

A.4.5 D-5. Recuperación tras incidentes

El servicio de recuperación tras incidentes tiene por objeto ayudar a restaurar la funcionalidad del sistema y su funcionamiento normal.

A.4.6 D-6. Notificación de incidentes

El servicio de notificación de incidentes tiene por objeto comunicar que se ha producido un incidente a los equipos de intervención y otros grupos interesados.

A.4.7 D-7. Informe de respuesta a incidentes

El servicio de informes de respuesta a incidentes tiene por objeto concluir y distribuir el informe de respuesta a incidentes cerrados (si las medidas de respuesta se prolongan, se delegarán al equipo de gestión estratégica del CCD (categoría A)). Si el personal del CCD necesita un informe sobre la situación actual durante la gestión de un incidente, este servicio le distribuirá un informe provisional.

A.5 Categoría E: Verificación y evaluación

A.5.1 E-1. Recopilación de información sobre la red

El servicio de recopilación de información sobre la red tiene por objeto recibir una descripción general de la configuración de red que se pretende proteger.

A.5.2 E-2. Inventario de activos

El servicio de inventario de activos tiene por objeto gestionar información pertinente para el inventario de sistemas, activos y aplicaciones que constituyen la infraestructura empresarial global dentro en el marco de la asistencia del CCD.

A.5.3 E-3. Evaluación de vulnerabilidades

El servicio de evaluación de vulnerabilidades tiene por objeto examinar redes, sistemas y aplicaciones para determinar vulnerabilidades y cómo pueden explotarse, así como recomendar formas de mitigar los riesgos.

A.5.4 E-4. Gestión de parches

Servicio de gestión de parches tiene por objeto dar soporte a la instalación de cualquier parche de seguridad necesario, mientras se mantiene la disponibilidad de tecnología de la información (IT).

A.5.5 E-5. Pruebas de penetración

El servicio de pruebas de penetración tiene por objeto descubrir vulnerabilidades de seguridad que podrían explotar atacantes y destacar los posibles métodos de poner en peligro la seguridad (por ejemplo, pruebas de penetración en función de la amenaza).

A.5.6 E-6. Evaluación de la capacidad de defensa contra ataques ATP

El servicio de evaluación de la capacidad de defensa contra peligros persistentes avanzados (ATP) tiene por objeto medir la capacidad de resistencia de la organización ante ataques específicos, al tiempo que se realizan pruebas de ingeniería social y formación específica sobre correo electrónico.

A.5.7 E-7. Evaluación de la capacidad de gestionar ciberataques

El servicio de evaluación de la capacidad de gestionar ciberataques tiene por objeto confirmar si las actividades de seguridad reales cuando se produce un supuesto ataque pueden activarse y si puede ponerse fin al incidente sin demora (denominado ejercicio de respuesta a ciberataques).

A.5.8 E-8. Observancia de políticas

El servicio de observancia de políticas tiene por objeto verificar la conformidad y el cumplimiento de las políticas de seguridad predefinidas.

A.5.9 E-9. Fortalecimiento

El servicio de fortalecimiento tiene por objeto optimizar la configuración del componente de IT a fin de identificar, evaluar y aplicar las configuraciones de seguridad de los sistemas y mitigar o eliminar los riesgos de ataques.

A.6 Categoría F: Recopilación, análisis y evaluación de inteligencia sobre amenazas

A.6.1 F-1. Análisis *post mortem*

El servicio de análisis *post mortem* tiene por objeto describir la resolución de un incidente para garantizar el examen y mejora de los procesos y herramientas para el personal del CCD.

A.6.2 F-2. Recopilación y análisis de inteligencia sobre amenazas internas

El servicio de recopilación y análisis de inteligencia sobre amenazas internas tiene por objeto recopilar información (inteligencia interna) sobre la respuesta a incidentes y el análisis en tiempo real.

A.6.3 F-3. Recopilación y evaluación de inteligencia sobre amenazas externas

El servicio de recopilación y evaluación de inteligencia sobre amenazas externas tiene por objeto recopilar información (inteligencia externa) sobre, por ejemplo, nuevas vulnerabilidades, tendencias

en ataques, comportamiento del malware, información sobre direcciones y dominios malignos del protocolo Internet.

A.6.4 F-4. Informe de inteligencia sobre amenazas

El servicio de información de inteligencia sobre amenazas tiene por objeto recopilar información sobre amenazas internas y externas y documentarla, con todos los detalles.

A.6.5 F-5. Utilización de inteligencia sobre amenazas

El servicio de utilización de inteligencia sobre amenazas tiene por objeto recopilar y divulgar información sobre amenazas para todas las categorías de respuestas de seguridad.

A.7 Categoría G: Desarrollo y mantenimiento de plataformas CCD

A.7.1 G-1. Implementación de arquitecturas de seguridad

El servicio de implementación de arquitecturas de seguridad tiene por objeto implementar la arquitectura de seguridad diseñada por el equipo directivo de estratégica del CCD (categoría A) mediante activos.

A.7.2 G-2. Funcionamiento básico de los activos de seguridad de la red

El servicio de funcionamiento básico de activos de seguridad de la red tiene por objeto explotar los dispositivos de red, por ejemplo, cortafuegos, sistemas de detección/prevención de intrusiones (IDS/IPS), cortafuegos para aplicación web (WAF) e intermediarios.

A.7.3 G-3. Funcionamiento avanzado de activos de seguridad de la red

El servicio de funcionamiento avanzado de activos de seguridad de la red tiene por objeto crear firmas personalizadas de la organización para productos con capacidad de detectar ataques, como IDS/IPS y WAF, y aplicarlos cuando la firma facilitada por el fabricante resulta insuficiente.

A.7.4 G-4. Funcionamiento básico de activos de seguridad periféricos

El servicio de funcionamiento básico de activos de seguridad periféricos tiene por objeto explotar los productos de medidas de protección, como el software antivirus software, en los puntos periféricos.

A.7.5 G-5. Funcionamiento avanzado de activos de seguridad periféricos

El servicio de funcionamiento avanzado de activos de seguridad periféricos tiene por objeto detectar toda actividad de programas sospechosa en el punto periférico que utiliza su producto de protección y recabar y analizar la situación de los registros, la ejecución de procesos, etc. En caso necesario, el servicio establece indicadores personalizados de riesgo para permitir la detección en el punto periférico.

A.7.6 G-6. Funcionamiento básico de productos de seguridad en la nube

El servicio de funcionamiento básico de productos de seguridad en la nube tiene por objeto explotar los servicios de seguridad en la nube.

A.7.7 G-7. Funcionamiento avanzado de productos de seguridad en la nube

El servicio de funcionamiento avanzado de productos de seguridad en la nube tiene por objeto crear firmas personalizadas de la organización para los servicios de seguridad en la nube con capacidades de detección de ataques. Si la firma facilitada por el fabricante resulta insuficiente, el servicio aplica firmas personalizadas.

A.7.8 G-8. Funcionamiento de herramientas de análisis profundo

El servicio de funcionamiento de herramientas de análisis profundo tiene por objeto explotar herramientas utilizadas en el análisis profundo, por ejemplo, análisis de malware y forense digital.

A.7.9 G-9. Funcionamiento básico de la plataforma de análisis

El servicio de funcionamiento básico de la plataforma de análisis tiene por objeto explotar la infraestructura analítica que almacena los datos de los requisitos necesarios y permite realizar el análisis rutinario, principalmente análisis en tiempo real, por ejemplo, la gestión de información y eventos de seguridad (SIEM).

A.7.10 G-10. Funcionamiento avanzado de la plataforma de análisis

El servicio de funcionamiento avanzado de la plataforma de análisis tiene por objeto realizar un análisis más detallado y preciso utilizando los propios sistemas de la organización para mantener los registros del sistema y los datos obtenidos de paquetes que los SIEM comerciales no pueden extraer, y diseñar algoritmos y lógica de análisis personalizados para esos datos, así como para los sistemas.

A.7.11 G-11. Funcionamiento de los sistemas del CCD

El servicio de funcionamiento de sistemas CCD tiene por objeto realizar las tareas necesarias para las operaciones de respuesta de seguridad, como las diversas herramientas de respuesta de seguridad antes descritas, la producción de diversos informes, la respuesta a consultas y el sistema de gestión de vulnerabilidades.

A.7.12 G-12. Evaluación de las herramientas de seguridad existentes

El servicio de evaluación de las herramientas de seguridad existentes tiene por objeto verificar los efectos sobre otros sistemas y operaciones, principalmente en términos de disponibilidad, cuando se actualiza o cambia la configuración de las herramientas de seguridad existentes.

A.7.13 G-13. Evaluación de nuevas herramientas de seguridad

El servicio de evaluación de nuevas herramientas de seguridad tiene por objeto diseñar e instalar nuevos activos de seguridad, cuando se requieren nuevas medidas en las actividades de seguridad.

A.8 Categoría H: Ayuda a la respuesta contra el fraude interno

A.8.1 H-1. Ayuda al análisis y respuesta contra el fraude interno

El servicio de ayuda al análisis y respuesta contra el fraude interno tiene por objeto ayudar a la organización a responder cuando se detecta fraude interno, mediante la organización de actividades a partir de los registros recabados por las actividades de seguridad.

A.8.2 H-2. Ayuda a detectar el fraude interno y prevenir la reincidencia

El servicio de ayuda a detectar el fraude interno y prevenir la reincidencia tiene por objeto analizar en detalle las actividades de fraude interno que se detecten, y examinar si es posible detectarlas a partir de los registros y, en su caso, implementar la lógica de detección.

A.9 Categoría I: Relación activa con partes externas

A.9.1 I-1. Sensibilización

El servicio de sensibilización tiene por objeto, precisamente, sensibilizar al personal pertinente de todo el CCD y que guarde relación con éste, promover la utilización de herramientas adecuadas, prácticas idóneas y políticas y recursos para garantizar la protección de los activos empresariales.

A.9.2 I-2. Educación y formación

El servicio de educación y formación tiene por objeto dar soporte a actividades de formación especializadas en el ámbito de la seguridad para el personal de las organizaciones que reciben el servicio del CCD.

A.9.3 I-3. Consultoría de seguridad

El servicio de consultoría de seguridad proporciona servicios de consultoría a diversas funciones de la empresa en materia de seguridad.

A.9.4 I-4. Colaboración con fabricantes de seguridad

El servicio de colaboración con fabricantes de seguridad tiene por objeto establecer una línea de comunicación directa con el proveedor de los productos o servicios de seguridad adquiridos, exigir respuestas cuando se detectan deficiencias en esta materia e intercambiar opiniones positivas sobre los aspectos a mejorar.

A.9.5 I-5. Servicio de colaboración con comunidades de seguridad externas

El servicio de colaboración con comunidades de seguridad externas tiene por objeto intercambiar información de manera proactiva mediante la participación en comunidades externas. Dicha información puede responder a las actividades de seguridad.

A.9.6 I-6. Presentación de informes técnicos

El servicio de presentación de informes técnicos tiene por objeto proporcionar informes sobre los resultados de las actividades de supervisión y gestión. Estas actividades ayudan a demostrar el nivel de seguridad de los sistemas y de la infraestructura de IT.

A.9.7 I-7. Informes de seguridad para ejecutivos

El servicio de presentación de informes de seguridad para ejecutivos tiene por objeto elaborar informes periódicos y análisis estadísticos para la alta dirección, a fin de señalar el nivel de seguridad y los indicadores del rendimiento operativo de la organización.

Bibliografía

[b-ITU-T X.1053] Recomendación UIT-T X.1053 (2017), *Código de prácticas sobre controles de seguridad de la información basada en la Recomendación UIT-T X.1051 para organizaciones de telecomunicaciones de pequeño o mediano tamaño*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2021